Notice of Allowability	Application No.	Applicant(s)	
	10/771,840	SHELEST ET AL.	
	Examiner	Art Unit	
	JUNG KIM	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *5/22/09*.

2. ☒ The allowed claim(s) is/are *1-10,12,14,15,17-20,22,23,25-45,47-51,53,56 and 60-63*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *10/5/09* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Jung Kim/
Primary Examiner, AU 2432

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given via e-mail correspondence by Attorney Edmund J. Walsh on 10/7/09.

The application has been amended as follows:

In the claims:

1. (Previously presented) A method for providing security in a computer system, comprising:

in a processor of a clean group server:

specifying a set of properties for use in determining if an item is clean;

in response to receiving an add request from an item, the add request containing evidence collected from the item relating to the presence or absence of the properties in the specified set of properties, evaluating the add request to determine if the evidence proves that the item has the specified set of properties;

determining from the evidence in the add request whether the item has the specified set of properties, and if so, designating the item as a member of a clean group by instructing a domain controller to add the item to the clean group, the domain controller configured to store information identifying network users and resources; and

managing access to a plurality of group policy objects through an active directory server, each of the group policy objects being associated with a

group defined by the domain controller, and the active directory server providing access to each of the plurality of group policy objects to items based on membership in a group defined by the domain controller such that only members of the clean group can read the group policy object;

wherein:

members of the clean group communicate using security associations; and

a group policy object of the plurality of group policy objects comprises parameters for security associations used by items of the clean group, whereby communication with items of the clean group is restricted to other items within the clean group.

2. (Previously presented) The method of Claim 1, wherein the item is a computer.

3. (Previously presented) The method of Claim 2, wherein when the computer is to be evaluated, a clean component is installed on the computer to perform compliance checks and to collect the evidence relating to the presence or absence of the properties in the specified set of properties.

4. (Original) The method of Claim 1, wherein a compliance check is performed at a selected time for an item to determine if the item has the specified set of properties.

5. (Original) The method of Claim 1, wherein one of the specified set of properties is whether all of the available updates have been installed.

6. (Original) The method of Claim 5, wherein the updates comprise at least one of security updates or service packs.

7. (Previously presented) The method of Claim 1, further comprising receiving a message sent by the clean component after the item fails a compliance check performed by the clean component wherein the message indicates that the item should not be in the clean group.

8. (Previously presented) The method of Claim 7, further comprising invalidating the clean group membership of the item in response to receiving the message.

9. (Previously presented) The method of Claim 8, wherein the clean group membership of the item comprises local actions including at least hiding the domain credentials of the item.

10. (Previously presented) The method of Claim 7, wherein if the compliance check fails, additional steps are taken including at least hiding cryptographic keys.

11. (Canceled)

12. (Previously presented) The method of Claim 1, wherein after the item is designated as a member of the clean group, a countdown is started and if another message is not received by the end of the countdown, the item is removed from the clean group.

13. (Canceled)

14. (Previously presented) The method of Claim 1, further comprising initiating a status check to determine if the items in the clean group still have the specified properties.

15. (Currently Amended) A system for managing security, comprising:

a network comprising a plurality of ports, at least a first portion of the ports being wireless ports and a second portion of the ports being Ethernet ports;

a clean group server connected on the network;

a domain controller connected on the network and configured to store information identifying network users and resources including a clean group indicating a group of computers and users that are more trusted than computers and users not included in the clean group;

a plurality of items coupled to the network, with a first portion of the plurality of items being coupled through a wireless port of the plurality of ports and a second portion of the plurality of items being coupled through an Ethernet port of the plurality of ports, each item comprising a clean runtime component, the clean runtime component being installed on the item and being able to communicate with the clean group server, the clean runtime component being configured to send an add request and a remove request to the clean group server, the add request including evidence to be evaluated by the clean group server for determining whether to add the item to a clean group;

wherein:

the clean group server is configured to determine whether the evidence sent by the clean runtime component is sufficient to prove that the item is in compliance with a security policy, and if so, to designate the item as a member of the clean group by instructing the domain controller to add the item to the clean group and to remove the item from the clean group in response to the remove request;

adding an item to the clean group comprises selectively providing access to information establishing security associations; and

communication among items in the clean group is performed using the security associations, thereby quarantining items outside the clean group from receiving information from or sending information to items within the clean group.

16. (Canceled)

17. (Previously presented) The system of Claim 15, wherein the plurality of items comprise computers.

18. (Previously presented) The system of Claim 15, wherein the clean runtime component is configured to perform self-governance actions in response to performing a compliance checks that indicates that the item does not meet selected criteria.

19. (Original) The system of Claim 18, wherein one of the criteria is whether selected available updates have been installed.

20. (Original) The system of Claim 19, wherein the updates comprise at least one of security updates or service packs.

21. (Canceled)

22. (Previously presented) The system of Claim 18, wherein the clean runtime component is configured to send the add request to the clean group server only after the self-governance compliance check passes.

23. (Previously presented) The system of Claim 15, wherein the clean group server is configured to, after designating the item as a member of the clean group, start a countdown;
and if another add request is not received by the end of the countdown, the clean group server is configured to remove the item from the clean group.

24. (Canceled)

25. (Previously presented) The system of Claim 15, wherein the clean group server is configured to initiate a compliance check for items to determine if they should remain in the clean group.

26. (Currently Amended) One or more computer-readable media having computer-executable components for providing security in a computer system, the computer-executable components comprising:

a clean runtime object for installation on a computer, wherein the clean runtime object, when executed, performs a compliance check to determine if the computer has a specified set of properties, and sends an add request containing evidence relating to whether the computer has the specified set of properties to a clean group server and when the clean runtime object subsequently determines that the computer does not have the specified set of properties, performs self governance actions that disable the computer from communication with the clean group; and

instructions for installation on a clean group server for processing the add request, wherein the instructions, when executed, cause the clean group server to instruct a domain controller configured to store information identifying network users and resources to add the computer as a member of a clean group upon receipt of an request, if the clean group server determines that the add request contains sufficient evidence to prove that the computer has the specified set of properties,

wherein:

adding the computer as a member of the clean group comprises selectively providing access to information establishing security associations; and

communication among items in the clean group is performed using the security associations, thereby quarantining computers outside the clean

group from receiving information from or sending information to computers within the clean group.

27. (Original) The media of Claim 26, wherein the compliance check is performed initially upon installation of the runtime object.

28. (Previously presented) The media of Claim 26, wherein the evidence indicates whether specified available updates have been installed on the computer.

29. (Previously presented) The media of Claim 28, wherein the specified available updates comprise at least one of security updates or service packs.

30. (Previously presented) The media of Claim 26, wherein after the add request is received by the clean group server, a countdown is started and if another message is not received by the end of the countdown, the clean group server instructs the domain controller to remove the computer from the clean group.

31. (Previously presented) The media of Claim 26, wherein the self governance action comprises at least one of erasing domain credentials, hiding domain credentials, hiding EFS keys or disabling EFS keys.

32. (Previously presented) The media of Claim 26, wherein the clean group server communicates with the runtime object to initiate a compliance check.

33. (Currently Amended) ~~A method of operating a computer for providing security in a computer system, comprising~~ The method of claim 1, wherein:

~~in a processor associated with the~~ the item is a computer; and[[:]]

~~evaluating a computer to determine if it has a specified set of properties specifying whether the computer is clean;~~

~~sending an add request to a clean group server when it is determined that the computer has the specified set of properties; and~~

the method further comprises, when the computer is a member of a clean group and it is determined that the computer does not have the specified set of properties, performing self governance action, the self governance action comprising at least one of erasing domain credentials, hiding domain credentials, hiding EFS keys or disabling EFS keys.

34. (Previously presented) The method of Claim 33, wherein:

based on whether or not the clean group server determines that the computer is in compliance, the clean group server disables or enables a computer domain account on a domain controller, the domain controller configured to store information identifying network users and resources; and

when a new computer domain account is to be added to the domain, the new domain account is placed in a disabled state until the associated computer is proved to the clean group server to be in compliance.

35. (Previously presented) The method of Claim 34, wherein when a new computer domain account is to be added to the domain, the domain join operation that creates the new computer domain account is predicated on proving that the computer is in compliance by requiring the clean group server to participate in the domain join operations.

36. (Previously presented) The method of Claim 34, wherein evaluating a computer comprises determining whether available updates have been installed on the computer.

37. (Previously presented) The method of Claim 34, wherein the computer periodically performs compliance checks.

38. (Previously presented) The method of Claim 34, wherein the clean group server periodically initiates a compliance check on the computer.

39. (Previously presented) A method for providing security in a computer system, comprising:

with a processor associated with each of a plurality of items, performing at least in part, a compliance check for the item;

communicating a result of the compliance check to a domain controller,

within the domain controller, for each of the plurality of items:

altering data storage to indicate that the item is not in the clean group when the compliance check for the item fails;

storing an indication that the item is in the clean group when the compliance check for the item passes;

selectively providing access to a collection of IPSec communication requirements and parameters based on membership in the clean group maintained by the domain controller; and

blocking access to the collection of IPSec communication requirements and parameters by items not within the clean group; and

limiting communicating among items in the clean group to communication using the IPsec communication requirements, thereby quarantining items outside the clean group from receiving information from or sending information to items within the clean group.

40. (Original) The method of Claim 39, wherein after an item passes a compliance check and is placed in the clean group, a countdown is started and if another compliance check is not passed by the end of the countdown, the item is removed from the clean group.

41. (Original) The method of Claim 39, wherein the item is a computer.

42. (Original) The method of Claim 39, wherein the item performs a compliance check.

43. (Original) The method of Claim 39, wherein a clean group server initiates a compliance check on the item.

44. (Original) The method of Claim 39, wherein the compliance check is performed by the item communicating with an update Web site to determine if updates are available for the item.

45. (Original) The method of Claim 44, wherein the item communicates with a clean group server to establish its membership in the clean group.

46. (Canceled)

47. (Previously presented) The method of Claim 39, wherein a compliance check is initiated by one or more of a client coming online, changes in client status/configuration, changes in network status/configuration, or changes to a compliance policy.

48. (Original) The method of Claim 39, wherein a clean group server communicates to non-compliant items how to get back into compliance.

49. (Original) The method of Claim 48, wherein the non-compliant items are directed to a Web site with online instructions to the user, and once the instructions are followed, another server-assisted compliance check is initiated.

50. (Original) The method of Claim 48, wherein the non-compliant items are instructed how to get into the compliant state automatically without requiring a user's involvement.

51. (Previously presented) The method of Claim 39, wherein an item is a user, and a
user's clean group membership is evaluated on the basis of whether each of a set of computers associated with the user is in compliance.

52. (Canceled)

53. (Previously presented) The method of Claim 39, wherein items within the clean group are given access to the collection of IPSec settings by binding active directory group policy to the clean group membership such that only members of the clean group can read the policy.

54-55. (Canceled)

56. (Previously presented) The method of Claim 39, wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group.

57-59.(Canceled)

60. (Previously presented) The method of Claim 1, further comprising designating the item as a member of a dirty group if the clean group server determines that the item does not have the specified set of properties.

61. (Previously presented) The system of Claim 15, wherein the clean group server is further configured to designate the item as a member of a dirty group if the

evidence sent by the clean runtime component is insufficient to prove that the item is in compliance with the security polio.

62. (Previously presented) The method of Claim 8, wherein the clean group membership of the item comprises local actions including at least erasing the domain credentials of the item.

63. (Previously presented) The method of Claim 7, wherein if the compliance check fails, additional steps are taken including at least logging out a privileged user.

Allowable Subject Matter

Claims 1-10, 12, 14, 15, 17-20, 22, 23, 25-45, 47-51, 53, 56 and 60-63 are allowed. The following is an examiner's statement of reasons for allowance: Applicant's arguments filed on 5/22/09 with respect to the rejection of claim 1 are persuasive. In particular, Applicant's arguments that the features related to security associations as defined in the claims (i.e. using security associations by the items added to the clean group to establish selective access to information, whereby communication among the items in the clean group is performed using the security associations, and thereby quarantining items outside the clean group from receiving information from or sending information to items within the clean group) is not suggested by the prior art of record is persuasive. For this reason, the claims are allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432